CLAIMS

1. (Currently Amended) A method for performing isolation of dropped packets, ~~in a computer network,~~ said method comprising:

receiving a request to isolate a dropped packet in a network ~~for analysis,~~ said request including a source node and a destination node;

mapping an expected routepath between the source node and the destination node ~~in response to said request for analysis,~~ said expected routepath including a probe;

creating a capture filter profile for said probe;

transmitting a request to said probe to perform data collection in response to said capture filter profile;

receiving a data log from said probe, said data log created by said data collection; ~~and~~

generating exception data including comparing said expected route to said data log; and

isolating the dropped packet by identifying a failing network element along the expected route in response to the exception data. ~~, wherein said exception data is generated in response to comparing said expected path and said data log.~~

2. (Currently Amended) The method of claim 1 wherein said request to isolate a dropped packet further includes a network protocol identifier.

3. (Currently Amended) The method of claim 1 wherein said request to isolate a dropped packet further includes restrictions on said expected routepath.

4. (Currently Amended) The method of claim 3 wherein said mapping is altered in response to said restrictions on said expected routepath.

5. (Original) The method of claim 1 wherein said capture filter profile includes said source node and said destination node.

6. (Original) The method of claim 5 wherein said capture filter profile further includes a network protocol identifier.

7. (Currently Amended) The method of claim 1 wherein said request to isolate a dropped packet ~~for analysis~~ is initiated programmatically by an agent in a network endpoint.

8. (Currently Amended) The method of claim 1 wherein said mapping an expected route~~path~~ is restricted based on network topology data.

9. (Original) The method of claim 1 wherein said data log comprises:

said source node, said destination node, a probe identifier, and a unique packet identifier.

10. (Original) The method of claim 1 further comprising:

transmitting a retransmission request to a specified node in response to said exception data.

11. (Original) The method of claim 1 further comprising:

transmitting a notification to a specified node in response to said exception data.

12. (Currently Amended) The method of claim 1 wherein said generating exception data further includes ~~comprises~~:

generating output data that includes the number of log entries corresponding to said probe and the number of log entries corresponding to a second probe, wherein said log entries are contained in said data log, and wherein said probe is a source probe and said second probe is a destination probe.

13. (Original) The method of claim 1 wherein said data log further comprises a frame sequence number.

14. (Currently Amended) The method of claim 13 wherein said generating exception data further includes~~comprises~~:

tracking a packet from said source node to said destination node using said frame sequence number; and

generating output data that includes the results of said tracking.

15. (Currently Amended) The method of claim 1 wherein said generating exception data further includes~~comprises~~:

tracking a packet from said source node to said destination node using a boolean expression; and

generating output data that includes the results of said tracking.

16. (Original) The method of claim 1 further comprising:

receiving said data collection request at said probe; and

programming said probe in response to said capture filter profile.

17. (Original) The method of claim 16 wherein said probe is in passive mode.

18. (Original) The method of claim 16 wherein said probe is in active mode.

19. (Original) The method of claim 18 wherein said capture profile contains instructions to cause said probe to simulate network errors.

20. (Original) The method of claim 16 further comprising:

capturing packet data for every packet received by said probe.

21. (Original) The method of claim 16 further comprising:

capturing packet data on a continuous basis at said probe.

22. (Original) The method of claim 1 further comprising:

capturing packet data for a time period specified by said capture filter profile;

writing a packet data identifier to said data log when said packet data matches said capture filter profile; and

transmitting said data log to requestor of said data collection.

23. (Currently Amended) A system for performing isolation of dropped packets in a ~~computer~~ network, said system comprising a problem isolation system in communication with said network, said problem isolation system implementing a process comprising:

receiving a request to isolate a dropped packet in the network ~~for analysis~~, said request including a source node and a destination node;

mapping an expected route between the source node and the destination node, ~~path in response to said request for analysis,~~ said expected route~~path~~ including a probe;

creating a capture filter profile for said probe;

transmitting a request to said probe to perform data collection in response to said capture filter profile;

receiving a data log from said probe, said data log created by said data collection; ~~and~~

generating exception data including comparing said expected route to said data log; and

isolating the dropped packet indentifying a failing network element along the expected route in response to the exception data, ~~, wherein said exception data is generated in response to comparing said expected path and said data log.~~

24. (Currently Amended) The system of claim 23 wherein said request to isolate a dropped packet further includes a network protocol identifier.

25. (Currently Amended) The system of claim 23 wherein said request to isolate a dropped packet further includes restrictions on said expected route~~path~~.

26. (Currently Amended) The system of claim 25 wherein said mapping is altered in response to said restrictions on said expected route~~path~~.

27. (Original) The system of claim 23 wherein said capture filter profile includes said source node and said destination node.

28. (Original) The system of claim 27 wherein said capture filter profile further includes a network protocol identifier.

29. (Currently Amended) The system of claim 23 wherein said request to isolate a dropped packet ~~for analysis~~ is initiated programmatically by an agent in a network endpoint.

30. (Currently Amended) The system of claim 23 wherein said mapping an expected route~~path~~ is restricted based on network topology data.

31. (Original) The system of claim 23 wherein said data log comprises:

said source node, said destination node, a probe identifier, and a unique packet identifier.

32. (Original) The system of claim 23 further comprising:

transmitting a retransmission request to a specified node in response to said exception data.

33. (Original) The system of claim 23 further comprising:

transmitting a notification to a specified node in response to said exception data.

34. (Currently Amended) The system of claim 23 wherein said generating exception data further includes~~comprises~~:

generating output data that includes the number of log entries corresponding to said probe and the number of log entries corresponding to a second probe, wherein said log entries are contained in said data log, and wherein said probe is a source probe and said second probe is a destination probe.

35. (Original) The system of claim 23 wherein said data log further comprises a frame sequence number.

36. (Currently Amended) The system of claim 35 wherein said generating exception data further includes~~comprises~~:

tracking a packet from said source node to said destination node using said frame sequence number; and

generating output data that includes the results of said tracking.

37. (Currently Amended) The system of claim 23 wherein said generating exception data further includes~~comprises~~:

tracking a packet from said source node to said destination node using a boolean expression; and

generating output data that includes the results of said tracking.

38. (Original) The system of claim 23 further comprising:

receiving said data collection request at said probe; and

programming said probe in response to said capture filter profile.

39. (Original) The system of claim 38 wherein said probe is in passive mode.

40. (Original) The system of claim 38 wherein said probe is in active mode.

41. (Original) The system of claim 40 wherein said capture profile contains instructions to cause said probe to simulate network errors.

42. (Original) The system of claim 38 further comprising:

capturing packet data for every packet received by said probe.

43. (Original) The system of claim 38 further comprising:

capturing packet data on a continuous basis at said probe.

44. (Original) The system of claim 23 further comprising:

capturing packet data for a time period specified by said capture filter profile;

writing a packet data identifier to said data log when said packet data matches said capture filter profile; and

transmitting said data log to requestor of said data collection.

45. (Currently Amended) A storage medium encoded with machine-readable computer program code for performing isolation of dropped packets ~~in a computer network~~, the storage medium storing instructions for causing a problem isolation system to implement a method comprising:

receiving a request to isolate a dropped packet in a network ~~for analysis~~, said request including a source node and a destination node;

mapping an expected routepath between the source node and the destination node, ~~in response to said request for analysis~~, said expected routepath including a probe;

creating a capture filter profile for said probe;

transmitting a request to said probe to perform data collection in response to said capture filter profile;

receiving a data log from said probe, said data log created by said data collection; ~~and~~

generating exception data including comparing said expected route to said data log; and

isolating the dropped packet by identifying a failing network element along the expected route in response to the exception data ~~, wherein said exception data is generated in response to comparing said expected path and said data log~~.

46. (Currently Amended) The storage medium of claim 45 wherein said request to isolate a dropped packet further includes a network protocol identifier.

47. (Currently Amended) The storage medium of claim 45 wherein said request to isolate a dropped packet further includes restrictions on said expected routepath.

48. (Currently Amended) The storage medium of claim 47 wherein said mapping is altered in response to said restrictions on said expected routepath.

49. (Original) The storage medium of claim 45 wherein said capture filter profile includes said source node and said destination node.

50. (Original) The storage medium of claim 49 wherein said capture filter profile further includes a network protocol identifier.

51. (Currently Amended) The storage medium of claim 45 wherein said request to isolate a dropped packetfor analysis is initiated programmatically by an agent in a network endpoint. .

52. (Currently Amended) The storage medium of claim 45 wherein said mapping an expected routepath is restricted based on network topology data.

53. (Original) The storage medium of claim 45 wherein said data log comprises:

said source node, said destination node, a probe identifier, and a unique packet identifier.

54. (Original) The storage medium of claim 45 further comprising instructions for causing the problem isolation system to implement:

transmitting a retransmission request to a specified node in response to said exception data.

55. (Original) The storage medium of claim 45 further comprising instructions for causing the problem isolation system to implement:

transmitting a notification to a specified node in response to said exception data.

56. (Currently Amended) The storage medium of claim 45 wherein said generating exception data further includescomprises:

generating output data that includes the number of log entries corresponding to said probe and the number of log entries corresponding to a second probe, wherein said log entries are contained in said data log, and wherein said probe is a source probe and said second probe is a destination probe.

57. (Original) The storage medium of claim 45 wherein said data log further comprises a frame sequence number.

58. (Currently Amended) The storage medium of claim 57 wherein said generating exception data further includes~~comprises~~:

tracking a packet from said source node to said destination node using said frame sequence number; and

generating output data that includes the results of said tracking.

59. (Currently Amended) The storage medium of claim 45 wherein said generating exception data further includes~~comprises~~:

tracking a packet from said source node to said destination node using a boolean expression; and

generating output data that includes the results of said tracking.

60. (Original) The storage medium of claim 45 further comprising instructions for causing the problem isolation system to implement:

receiving said data collection request at said probe; and

programming said probe in response to said capture filter profile.

61. (Original) The storage medium of claim 60 wherein said probe is in passive mode.

62. (Original) The storage medium of claim 60 wherein said probe is in active mode.

63. (Original) The storage medium of claim 62 wherein said capture profile contains
instructions to cause said probe to simulate network errors.

64. (Original) The storage medium of claim 60 further comprising:
capturing packet data for every packet received by said probe.

65. (Original) The storage medium of claim 60 further comprising:
capturing packet data on a continuous basis at said probe.

66. (Original) The storage medium of claim 45 further comprising instructions for causing the problem isolation system to implement:
capturing packet data for a time period specified by said capture filter profile;
writing a packet data identifier to said data log when said packet data matches said capture filter profile; and
transmitting said data log to requestor of said data collection.